PATENT

Docket Number: 4208-4070

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION FOR:

A METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR SECURE TICKETING IN A COMMUNICATIONS DEVICE

INVENTORS:

OLLI IMMONEN
NADARAJAH ASOKAN
PANU MARKKANEN

Morgan & Finnegan, L.L.P
345 Park Avenue
New York, New York 10154-0053
(212) 758-4800
(202) 857-7887

Attorneys for Applicants

PATENT Docket Number: 4208-4070

A METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR SECURE TICKETING IN A COMMUNICATIONS DEVICE

CROSS-REFERENCE TO RELATED PATENT APPLICATION

[0001] This application is a continuation-in-part of application No. 09/978,701 titled, “A METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR INTEGRITY-PROTECTED STORAGE IN A PERSONAL COMMUNICATION DEVICE” filed on October 18, 2001, which is incorporated herein by reference.

FIELD OF THE INVENTION

[0002] This invention relates to a method, system and computer program product for copy protection. The invention further relates to copy protection for use in communication devices.

BACKGROUND OF THE INVENTION

[0003] The use of communication devices in every aspect of our daily lives has increased dramatically over recent years. With the proliferation of communication devices such as personal trusted devices, it has become more and more important to protect the critical data used by the device. One popular feature of personal trusted devices is the use of electronic vouchers or tickets. A user of a personal trusted device may receive and store electronic tickets in the memory of the device and use them as payment for services provided by a third-party. For example, electronic tickets can be used to pay for admission to public events, riding, public transportation, etc. The tickets are generally paid for in advance and credited to the user of the terminal by a trusted third-party, or they are charged from the user by the operator through phone billing. However, although the use of electronic ticketing provides increased flexibility for the average consumer, it raises new security issues for third-parties that issue the electronic tickets.

[0004] For example, the issuer of a ticket may want to prevent a user of a personal trusted device from modifying or duplicating an issued ticket to travel by public transportation. The right to travel on public transportation is delivered to a user as an electronic ticket that specifies a number of uses. However, if a user can some how modify or duplicate the ticket, the user may make an indefinite number of trips without having to pay the issuer of the ticket for each use.

[0005] Various methods of cryptography have been used to protect against undetectable modification or duplication of critical data. Cryptography involves the encoding or encrypting of digital data to render it incomprehensible by all but the intended recipients. In other words, the data is encrypted and the decryption key is delivered to those terminals or users that have paid to use the data. To this end, cryptographic systems can be used to preserve the privacy and integrity of the data by preventing the use and alteration of data by unauthorized parties. In addition to encryption, authentication of the origin of data is used in order to make sure that e.g., only a party who has the right key can generate the right signature of message authentication code (MAC).

[0006] For example, a plaintext message consisting of digitized sounds, letters and/or numbers can be encoded numerically and then encrypted using a complex mathematical algorithm that transforms the encoded message based on a given set of numbers or digits, also known as a cipher key. The cipher key is a sequence of data bits that may either be randomly chosen or have special mathematical properties, depending on the algorithm or cryptosystem used. Sophisticated cryptographic algorithms implemented on computers can transform and manipulate numbers that are hundreds or thousands of bits in length and can resist any known method of unauthorized decryption. There are two basic classes of cryptographic algorithms: symmetric key algorithms and asymmetric key algorithms.

[0007] Symmetric key algorithms use an identical cipher key for both encrypting by the sender of the communication and decrypting by the receiver of the communication. Symmetric key cryptosystems are built on the mutual trust of the two parties sharing the cipher key to use the cryptosystem to protect against distrusted third parties. A well-known symmetric key algorithm is the National Data Encryption Standard (DES) algorithm first published by the National Institute of Standards and Technology. See Federal Register, Mar. 17, 1975, Vol. 40, No. 52 and Aug. 1, 1975, Vol. 40, No. 149. The sending cryptographic device uses the DES algorithm to encrypt the message when loaded with the cipher key (a DES cipher key is 56 bits long) for that session of communication (the session key). The recipient cryptographic device uses an inverse of the DES algorithm to decrypt the encrypted message when loaded with the same cipher key as was used for encryption.

[0008] Asymmetric key algorithms use different cipher keys for encrypting and decrypting. In a cryptosystem using an asymmetric key algorithm, the user makes the encryption key public and keeps the decryption key private, and it is not feasible to derive the private decryption key from the public encryption key. Thus, anyone who knows the public key of a particular user could encrypt a message to that user, whereas only the user who is the owner of the private key corresponding to that public key could decrypt the message. This public/private key system was first proposed in Diffie and Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Nov. 1976, and in U.S. Pat. No. 4,200,770 (Hellman et al.), both of which are hereby incorporated by reference. The most commonly used public key system for encryption and signing is RSA public key cryptography. RSA is a public key encryption algorithm that was invented in 1977 and named after its inventors Rivest, Shamir and Adleman. A more recent development in the area of cryptography is the digital signature. The digital signature is a mechanism that does not involve secrets but it protects data from undetected change by associating the data with the owner of a specific private key. Thus, a digital signature tends to be extremely difficult to forge.

[0009] While standard cryptographic methods can be used to implement most aspects of secure ticketing, protection against copying requires that the ticket collecting device retain state information about previously used tickets. However, in an off-line ticket collection scenario with many different collecting devices (e.g., one on each bus), there is no common trusted storage shared by all collecting devices.

[0010] Therefore, it is desirable to provide a system, method and computer program product that provides secured ticketing in a personal communications device, such as e.g., personal trusted device using a tamper-resistant security element. The system, method and computer program product of the embodiment of present invention disclosed herein address this need.

SUMMARY OF THE INVENTION

[0011] A method, system and computer program product for preventing duplication of critical data utilized by tickets, which are utilized with a communications device.

[0012] The method, system and computer program product of the embodiments of the present invention present invention use a tamper-resistant security element and cryptography for the secure transmission and storage of tickets used by communication devices.

[0013] It is contemplated by an embodiment of the invention that communication between a communications device, a tamper-resistant security element, and a third party device is achieved using at least two basic communication protocols: 1) request and store ticket protocol, and 2) use ticket protocol.

[0014] It is contemplated by an embodiment of the invention that communication between elements in the communication device and third-party devices also includes a check ticket protocol.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying figures illustrate the details of the method, system and computer program product of an embodiment of the present invention for implementing secure ticketing in a communication device. Like reference numbers and designations in these figures refer to like elements.

[0016] Fig. 1 is a network diagram that illustrates a communication device in accordance with an embodiment of the invention.

[0017] Fig. 2 is a network diagram that illustrates the use of cryptography in accordance with an embodiment of the present invention.

[0018] Fig. 3 is a detailed diagram that illustrates a communication device in accordance with an embodiment of the present invention.

[0019] Fig. 4 is a flow diagram that illustrates the execution of the request and store ticket protocol in accordance with an embodiment of the invention.

[0020] Fig. 5 is a flow diagram that illustrates the execution of a use ticket protocol in accordance with an embodiment of the invention.

[0021] Fig. 6 is a flow diagram depicting the execution of a check ticket protocol in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0022] Fig. 1 is an embodiment of the present invention that illustrates a system for secured ticketing in a communications device. The personal trusted device **100** is a wireless handheld telephone, a satellite telephone, a personal digital assistant, or a bluetooth device or any other communications device. The personal trusted device (PTD) **100** includes a mobile equipment (ME) **102** and a secure element **106**. The mobile equipment **102** includes an internal storage device **101**, operating system **107** and central processor **210**. The external memory **106** includes a tamper-resistant security element (SE) **103**. Tamper-resistant is a term known in the art that defines a secure section or memory or storage. A tamper-resistant boundary makes it difficult for an attacker to get at an internal element or data within a secure section. An example of security element framework is an ISO/IEC 7816, identification card-integrated circuit(s) cards with contacts, and utilizing AID (application identifier) defined in ISO/IEC 7816 -with added functionality according to the embodiment of the invention. Other examples include secure MMC (Multimedia Card), embedded hardware, etc. The security element **103** is an electronic card such as smartcard, flashcard or WIM card that is received by the personal trusted device **100** and completely removable.

[0023] The mobile equipment **102** is in communication with the security element **103** via the bus **109**. Additionally, the personal trusted device **100** is in communication with third-party devices **140, 150** and **160** for receiving and transmitting electronic tickets via a connection **111**, which is typically, but not necessarily a wireless connection. Examples of the communication links may comprise e.g., GSM, GPRS, WCDMA, DECT, WLAN, PSTN, ISDN, ADSL and xDSL connections or the DOCSIS return channel in a cable TV environment, or any short range connection like Bluetooth, IrDA. Communication between the mobile equipment **102**, external memory **106** and third-party devices **140, 150** and **160** is achieved using various protocols executed by the operating system **107** and the central processor **210**. The protocols used for communication between the mobile equipment **102**, the security element **103** and third-party devices **140, 150, 160** include, in an embodiment, a request and store ticket protocol, a use ticket protocol and a check ticket protocol.

[0024] The personal trusted device **100** in Fig. 1 is connectable to, for example, a wireless network **116** via a transmitted signal such as a frequency-modulated signal from the personal trusted device **100** and received by a base station antenna **114**. It will be understood that the mobile equipment **102** may be provided also with the short range connectivity in addition to the mobile communication activity. From the wireless network **116**, the personal trusted device can be connected to various third-party devices **140, 150, 160** via a network **130** and a wireless network switch **120**. The network **130** can be a server, Intranet, Internet, public switching network (PSTN), public exchange (PBX) or the like. The user (not shown) of the device can communicate with the personal trusted device **100** using the display **212** and keypad **104** and via the bus **109.**

[0025] The third-party devices **140, 150, 160** are in an embodiment of the invention devices that are connected to computer servers, or to a computer network **130** or the like, which are owned or operated by a third-party and are used to process and monitor the use of third-party services by the user of the personal trusted device **100**. By way of example, the third-party provides a service to the user of the personal trusted device **100** that may relate to payment for public transportation, admission to a public event, etc. The user of the personal trusted device **100** pays for the service in advance and is then credited with an electronic ticket by the issuing device **140** via the connection **111** and the remaining network illustrated in Fig. 1. Occasionally, it is necessary for the third party to check or verify the number of electronic tickets stored in the personal trusted device, which is done using a checking device **160**. After receiving the electronic tickets, the user can use or redeem the tickets with the third party by sending the ticket to the collecting device **150**.

[0026] The security element **103** and the ticket used for secure ticketing are further described herein using a simplified example. A secure element **103** comprises a plurality of counters, a certificate and a pair of cryptographic keys. Every counter comprises a unique counter identification, counter ID and a counter value. The counter is zero when the counter is created and initiated. The counter value represents the number of uses of a ticket and is incremented every time, when the associated ticket is used.

Security Element:

-Certificate (issued by the manufacturer)

-A Cryptographic Key Pair (public key, private key), e.g., RSA key pair.

-Counters:

	Counter ID	Counter Value
[counter 1]	12345	5
[counter 2]	12346	3
[counter 3]	12347	1
[counter n]	12349	0

[0027] In this example, the security element comprises n counters, each associated with an issued ticket. The ticket itself is stored in the mobile equipment in a first storage device. The counter 1 has a unique identification number "12345" and the value of the counter 1 is "5," which means that the associated ticket has been used for five (5) times. Correspondingly, the ticket associated with the counter ID "12346" has been used three (3) times. The public key for this security device in this example is "12abc." Each of the tickets issued by an issuing device and stored in the first storage device of mobile equipment can be described as follows:

	Counter ID	Public Key	N	Additional Information	Signature
[ticket 1]	12345	12abc	10	Greyhound	3458a
[ticket 2]	12346	12abc	10	Suburban train	25f72
[ticket 3]	12347	12abc	3	Cinema "stardust"	807
[ticket n]	12349	12abc	1	State Filharmonic (seat 234; May 23, 2002)	b62gp

[0028] Every ticket has a signature, which can be verified using the public key of the issuer of the ticket. Because all tickets in the example have been issued by different issuing devices they have different signatures and the signatures can be verified using the public key of the issuing device. When the ticket is presented to a collecting device, the collecting device checks the validity of the ticket by verifying the signature in the ticket. The first ticket is associated with the counter ID "12345" and it is issued by "Greyhound Co." for ten (10) uses. Correspondingly, the ticket associated with the counter ID "12347" is issued by the cinema company "stardust" for three (3) uses. The additional information can specify the rights as in the example for the ticket issued by the "state Filharmonic" to a certain date and to a certain seat. If the "counter value" stored in the security element is compared with the value "N" in the ticket, it can be seen that the user having a ticket with a counter ID "12345" has used "Greyhound Co." services five (5) times and can still use the services of "Greyhound Co." for another five (5) times.

[0029] Figure 2 illustrates in more detail the cyptography for implementing secured ticketing by mobile equipment **102**, the security element **103**, and third-party devices **140**, **150**, **160** in accordance with an embodiment of the invention. The mobile equipment **102** stores ticket data **101A** in the internal storage device **101** of the personal trusted device **100**. The ticket data **101A** corresponds to the valid tickets received by the issuing device **140** and not yet redeemed by the user. More importantly, the external security element **103** is trusted by the third parties involved. The security element **103** uses the public key **103C** and a corresponding private key **103D** only to implement a trusted counter application. Additionally, the mobile equipment **102** may also request a manufacturer certificate **103B** to ensure that the external security device **103** is issued by a trusted manufacturer.

[0030] The security element **103** is used to store a plurality of monotonically increasing or decreasing counters. Each of the counters consists of a unique identifier counter ID **103A** and an associated current value that represents uses of an electronic ticket, which are redeemable by a user of the personal trusted device **100**. For example, each time an electronic ticket is redeemed the counter value is updated and stored in the security element **103** of the personal trusted device **100**. As mentioned previously, the security element **103** includes public and private keys **103C**, **103D** and a card certificate **103B**.

[0031] The third-party devices contemplated by the invention include issuing devices **140**, collecting devices **150**, and checking devices **160**. The issuing device is used to send electronic tickets to the user of the personal trusted device **100** after the payment of third-party services. Additionally, the collecting device **150** is used to redeem electronic tickets and the checking device **160** is used to periodically check if the user is in possession of a correctly redeemed ticket. Each of the third-party devices includes public and private keys **140A, 140B, 150A, 150B, 160A, 160B**. It is presumed that the personal trusted device **100** is trusted by the user but is not trusted by the third-party devices. Thus, each of third-party devices can use public and private keys **140A, 140B, 150A, 150B, 160A, 160B** to encrypt critical data for secure communication of electronic tickets with the personal trusted device **100**. The keys **140A, 140B, 150A, 150B, 160A, 160B** in the third-party devices can be encryption keys, signature keys or master keys. A master key is a common symmetric key shared by all issuing, collecting and checking devices **140, 150, 160.**

[0032] Fig. 3 is another embodiment of the present invention that illustrates a system for secured ticketing in a personal trusted device **100**. Fig. 3 differs from Fig. 1 in that the system includes a plurality of collection devices **150**. A user of the personal trusted device **100** can redeem electronic tickets issued by issuing device **140** at any collection device **150** owned by a third-party. In other words, the user sends an electronic ticket to a collection device **150** via the connection **111** and the remaining network of Fig. 1. It is also contemplated by the invention that the system can also include more than one issuing device **140** or more than one checking device **160** (not shown).

[0033] Figs. 4-6 illustrate an embodiment of the invention using protocols for secured ticketing in the personal trusted device **100** through communication between the mobile equipment **102**, the security element **103** and third party devices **140, 150, 160.**

[0034] Fig. 4 illustrates the steps involved for executing the request and store ticket protocol that is used for receiving and storing electronic tickets in the personal trusted device **100**. Initially, in step **S1** mobile equipment **102** requests the card certificate **103B**

stored in the external security element **103**. In another embodiment of the invention the card certificate itself is not stored in the security element **103**, but a pointer to the card certificate in the form of an URL address is stored in the security element **103**, wherein in step **S1** the mobile equipment **102** requests the card certificate from the URL. As mentioned previously, the certificate ensures that the security element **103** is issued by a trusted manufacturer. In step **S2** the security element **103** sends a card certificate **103B**, which is verified by the mobile equipment **102** as a compliant card using a certificate chain. Two certificates can be used in order for mobile equipment **102** to verify that the security element **103** possesses a compliant card certificate **103B**. For example, a certificate issued by the mobile equipment **102** to the manufacturer of the security element **103**, and a compliant card certificate issued by the manufacturer of the external security element **103** to the security device **103** itself. In step **S2**, the security element **103** also sends a public key **103C** or the card certificate **103B**. In step **S3**, the mobile equipment **102** issues a create counter request to create a new counter to correspond to the electronic ticket that is to be received and later redeemed and/or checked by third party devices **140, 150, 160**. In step **S4**, the security element **103** sends a counter ID that is used to uniquely identify a counter. In step S5, the mobile equipment **102** forwards the counter ID, and the public key and manufacturer certificate of the external security element **103** to the issuing device **140**. In step **S6**, the issuing device **140** creates a ticket. The ticket is a signature on authenticator data for the issuing device consisting of the counter ID **103A**, the public key **103C** and a number of uses N (not shown) of the ticket created. The number of uses is, for example, the number of uses allowed by the user for this ticket (e.g., 10-use ticket will have N=10). In addition, the authenticator data may include other relevant information, such as e.g., a seat number and/or a date and/or time related to the ticket, to be used by the personal trusted device **100**. By way of example, the ticket issued using the issue ticket protocol resembles ticket = Sig_Issuer(counterID/Public Key_Device **103**/N/other_info). In step **S6**, the ticket is sent to the mobile equipment **102** and stored in the internal storage device **101**.

[0035] If the issuing device **140** wants to further determine the authenticity of the security element **103**, and the ticket data **101A**. The issuing device **140** can issue a challenge to the mobile equipment **102** prior to creating the ticket. In this case, the mobile equipment **102** responds to the challenge by invoking a read counter request and returns a signature on authenticator data for the external security element **103** that includes the current counter value. If the signature and data are verified as correct, then the issuing device **140** will create and issue a valid ticket.

[0036] Fig. 5 illustrates the use ticket protocol in accordance with an embodiment of the invention. In step **S7**, the mobile equipment **102** redeems a ticket by sending a ticket to a collecting device **150** using, for example, the network connections illustrated in Fig. 1. In step **S8**, the collecting device **150** responds by sending a challenge to the mobile equipment **102**. In step **S9**, the mobile equipment **102** invokes an update counter for the counter ID corresponding to the ticket by sending a request to the security element **103** with the challenge sent by the collecting device **150** as an input parameter. As a result of the update request, the security element **103** updates the counter by incrementing or decrementing the counter value and generating an authorization token. The authorization token is a signature on authenticator data that contains in addition to other parameters, the counter ID, current value of the counter and public key **103C**. By way of example, the authorization token using the use protocol resembles AuthToken = Sig_Device **103**(Update_Response/CounterID/Challenge/Current_Value).

[0037] In step **S10**, the security element **103** returns the authority token to the mobile equipment **102**. In step **S11**, the mobile equipment **102** forwards the authorization token to the collecting device **150**. The collecting device **150** verifies the signature on the authorization token using a public key **103C** of the security element **103** and then checks the current counter value. The collecting device **150** checks the counter value to ensure that the counter value is less than or equal to N. In step **S12**, the collecting device **150** sends an acknowledgment of the counter value to the mobile equipment **102**.

[0038] The collecting device **150** may optionally send a validated ticket containing the counter ID **103A**, the public key **103C** and the current counter value and any other additional information to the mobile equipment **102**. The validated ticket would then be received by the mobile equipment **102** and stored in the internal storage device **101**.

[0039] Once the ticket is fully used up (e.g., counter value = N), the mobile equipment **102** can delete the counter. In step **S13**, the mobile equipment **102** sends a request to delete the counter to the external security element **103**. The mobile equipment **102** sends the request along with the counter ID **103A**. In step **S14**, the security element **103** responds by returning the result of the delete counter request. For example, the response is either success or failure.

[0040] The ticket issued by an issuing device **140** can also include a multi-use ticket. In the case of a multi-used ticket, the mobile equipment **102** may send both the original ticket as well as the set of validated tickets obtained from the collecting device **150**. The collecting device **150** would then use the additional information (i.e., validated tickets) to make decisions with regard to access control. Additionally, a collecting device **150** may also replace an old ticket or issue a new ticket. To this end, a collecting device **150** also acts as an issuing device **140**.

[0041] Fig. 6 illustrates the check ticket protocol in accordance with an embodiment of the invention. In step **S15**, the mobile equipment **102** sends a ticket to the checking device **160**. In step **S16**, the checking device **160** sends a challenge to the mobile equipment **102**. In step **S17**, the mobile equipment **102** invokes a read counter for the corresponding counter ID by sending a read counter request to the external security element **103** using the challenge of the checking device **160** as an input parameter. In step **S18**, the security element **103** sends an authorization token that contains the current value of the counter to the mobile equipment **102**. By way of example, the authorization token sent using the check ticket protocol is AuthToken = Sig_Device **103** (Read_Response/CounterID/Challenge/current_value). In step **S19**, the mobile equipment **102** forwards the authorization token from the security element **103** to the checking device **160**. The checking device **160** checks the current value of the counter using the public key **103C**. In step **S20**, the checking device **160** sends an acknowledgment to the mobile equipment **102** indicating the status of the check. The status of the check by the checking device **160** is either success or failure.

[0042] In an alternative embodiment, in the use ticket protocol, step **S7** may be combined with step **S11**, and similarly in the check ticket protocol, step **S15** may be combined with step **S19**.

[0043] In another embodiment, the challenge value (such as in step **S8** of the use ticket protocol, or step **S16** of the check ticket protocol) may be a periodically changing broadcast challenge that is common to all the user devices running the protocol at a given time period.

[0044] In another embodiment of the present invention, the ticket issued is a signature on authenticator data that includes an encryption using a master key that can be used to transport a reference to the ticket and its MACKey from the issuing devices **140** to the collecting devices **150**, and from collecting device **150** to checking device **160**. All of the entities share the master key for secured communication of data.

[0045] In yet another embodiment, the ticket includes a set of encryptions, one for each collector **150**. Each individual encryption may be a public key encryption or shared key encryption. The latter is considered desirable if the number of collectors is small (< 10) because it results in smaller tickets.

[0046] In yet another embodiment, the collecting device **150** can contact an issuing device **140** via a secure channel and obtain a key. In this case, the key may be an index key to a key database of the issuing device. This is considered desirable in the case of multi-use tickets where the number of uses is very high. In this embodiment, each collecting device **150** needs to contact the issuing device **140** only once for a given ticket.

[0047] Additionally, as an alternative to computing an authorization token, a MAC can be used as an authentication method. For example, the MAC can be a code function such as HMAC-MD5 with the public key **103C** as the key of the MAC function. By way of example, the issue ticket protocol would change as follows if a MAC function is used as an authentication method. In response to a ticket request, the issuing device **140** creates a ticket and also computes an encypted key (EncKey) by encrypting the counter ID and MAC key (MACKey) using the public encryption key **103C** for the security element **103**. By way of example, the ticket issued using the issue protocol and the MAC is Ticket = Sig_Issuer (CounterID/Public Key_Device **103**/N/Other_Info), EncKey = Enc_device **103**(CounterID/MACKey). The mobile equipment **102** inputs the received encrypted key EncKey into security element **103**. The security element **103** recovers the MACKey from the EncKey and sets the authentication method to MAC using MACkey. The security element **103** sends an acknowledgment to the mobile equipment **102**. Other protocols would have similar changes as noted above if a MAC is used as an authentication method.

[0048] Although illustrative embodiments have been described herein in detail, it should be noted and understood that the descriptions and drawings have been provided for purposes of illustration only and that other variations both in form and detail can be added thereupon without departing from the spirit and scope of the invention. The terms and expressions have been used as terms of description and not terms of limitation. There is no limitation to use the terms or expressions to exclude any equivalents of features shown and described or portions thereof.